Create a Strong Password and Evaluate Its Strength

Objective: Understand what makes a password strong and test it against password strength tools.

I created 5 different passwords with varying complexity to compare their strengths.

- theertha123
- theertha!
- theertha@123
- theertha@123!
- .T@!u7bK$e9#P@1x

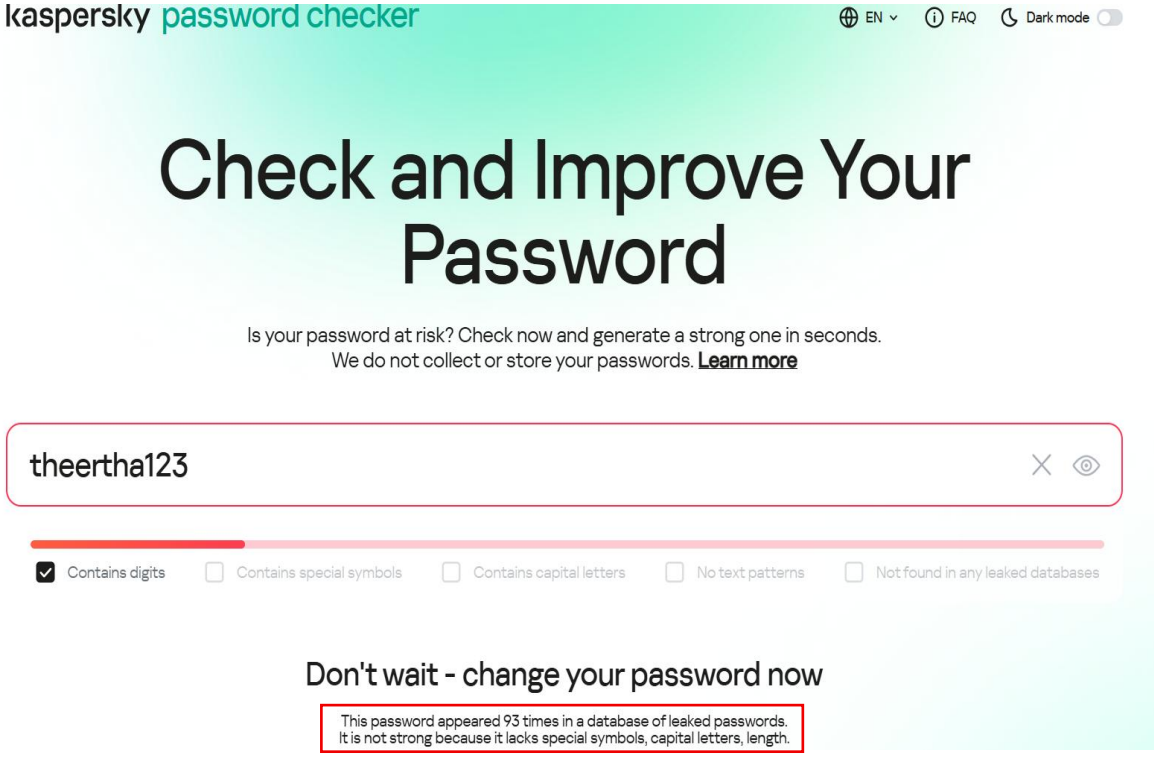
To understand password complexity better, I varied:

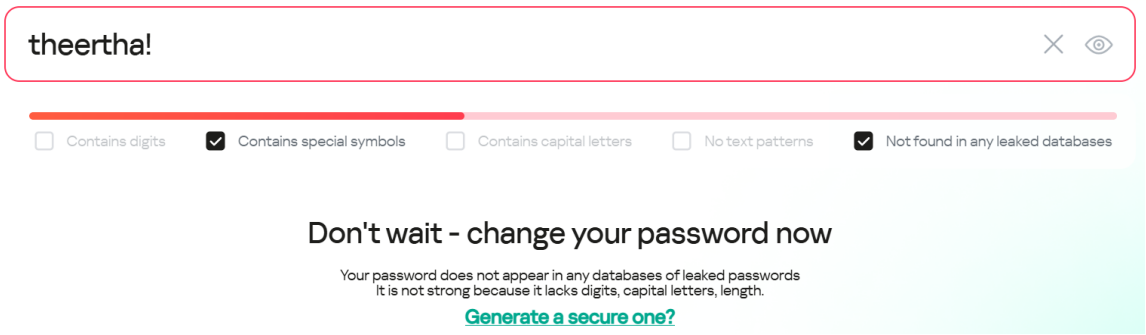
- Character types: lowercase, uppercase, numbers, and symbols.
- Password length: from short (9 characters) to strong (16+ characters).
- The strongest password .T@!u7bK$e9#P@1x includes all character types and is 16+ characters long, making it highly secure.

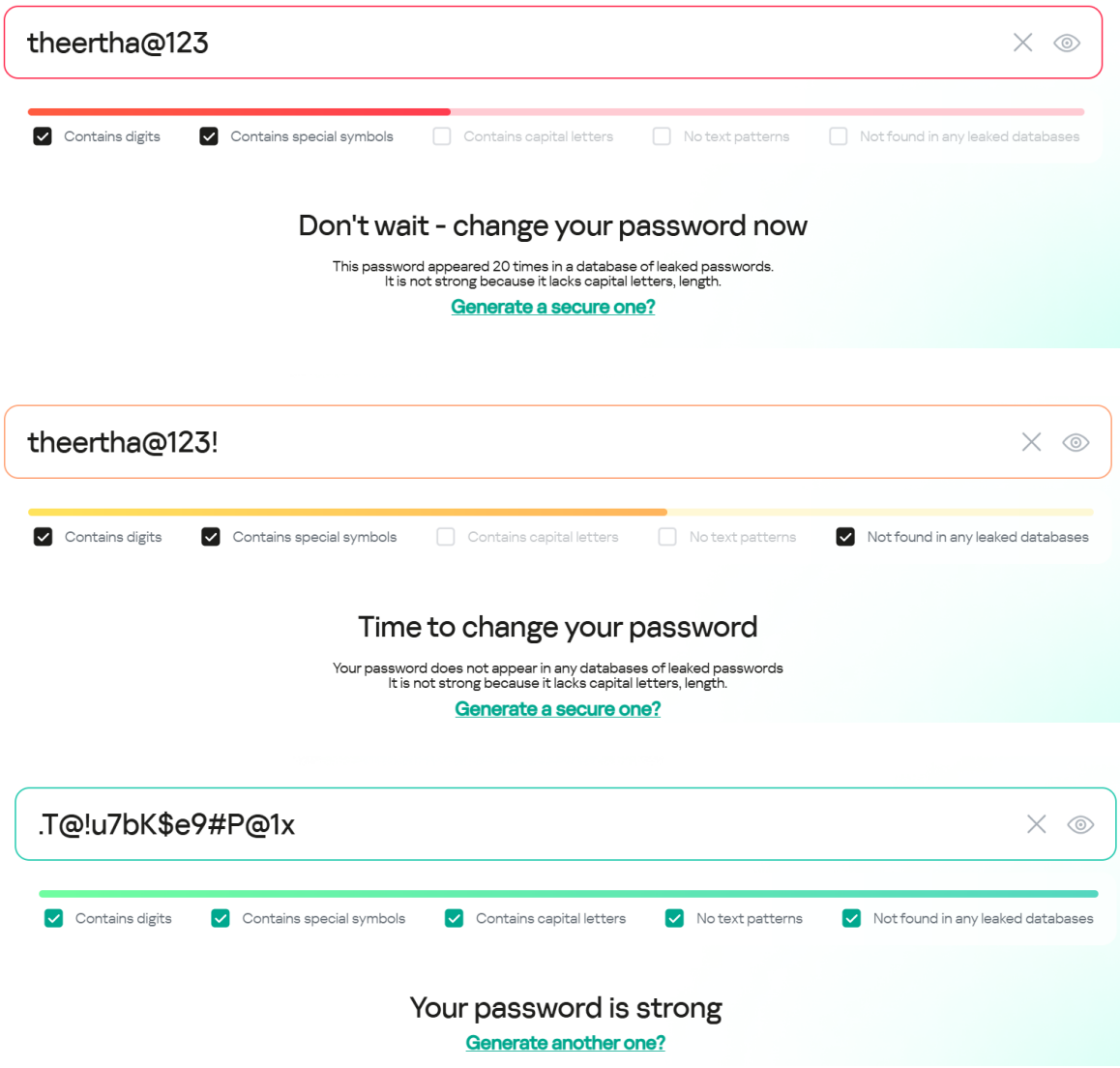
I used the following online password strength checkers:

- Kaspersky Password Checker
- PasswordMeter

These tools analyzed the structure of the passwords and provided strength scores and feedback.







The Password Meter

Test Your Password		Minimum Requirements
Password:	theertha123	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:		
Score:	44%	
Complexity:	Good	

Additions		Type	Rate	Count	Bonus
+	Number of Characters	Flat	+(n*4)	11	+ 44
-	Uppercase Letters	Cond/Incr	+((len-n)*2)	0	0
+	Lowercase Letters	Cond/Incr	+((len-n)*2)	8	+ 6
+	Numbers	Cond	+(n*4)	3	+ 12
-	Symbols	Flat	+(n*6)	0	0
+	Middle Numbers or Symbols	Flat	+(n*2)	2	+ 4
-	Requirements	Flat	+(n*2)	3	0

Test Your Password		Minimum Requirements
Password:	theertha!	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	28%	
Complexity:	Weak	

Additions		Type	Rate	Count	Bonus
✓	Number of Characters	Flat	+(n*4)	9	+ 36
✗	Uppercase Letters	Cond/Incr	+((len-n)*2)	0	0
✓	Lowercase Letters	Cond/Incr	+((len-n)*2)	8	+ 2
✗	Numbers	Cond	+(n*4)	0	0
✓	Symbols	Flat	+(n*6)	1	+ 6
✗	Middle Numbers or Symbols	Flat	+(n*2)	0	0
✗	Requirements	Flat	+(n*2)	3	0

Test Your Password		Minimum Requirements
Password:	theertha@123	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	66%	
Complexity:	Strong	

Test Your Password		Minimum Requirements
Password:	theertha@123!	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	80%	
Complexity:	Very Strong	

Additions		Type	Rate	Count	Bonus
✓	Number of Characters	Flat	+(n*4)	13	+ 52
✗	Uppercase Letters	Cond/Incr	+((len-n)*2)	0	0
✓	Lowercase Letters	Cond/Incr	+((len-n)*2)	8	+ 10
✓	Numbers	Cond	+(n*4)	3	+ 12
✓	Symbols	Flat	+(n*6)	2	+ 12
✓	Middle Numbers or Symbols	Flat	+(n*2)	4	+ 8
✓	Requirements	Flat	+(n*2)	4	+ 8

Test Your Password		Minimum Requirements
Password:	T@!u7bK$e9#P@1x	• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☐	
Score:	100%	
Complexity:	Very Strong	

Additions		Type	Rate	Count	Bonus
✓	Number of Characters	Flat	+(n*4)	15	+ 60
✓	Uppercase Letters	Cond/Incr	+((len-n)*2)	3	+ 24
✓	Lowercase Letters	Cond/Incr	+((len-n)*2)	4	+ 22
✓	Numbers	Cond	+(n*4)	3	+ 12
✓	Symbols	Flat	+(n*6)	5	+ 30
✓	Middle Numbers or Symbols	Flat	+(n*2)	8	+ 16
✓	Requirements	Flat	+(n*2)	5	+ 10

From the password evaluations using strength checker tools, the following best practices were identified to ensure password security:

1. **Avoid Short or Common Passwords**
   Short passwords like theertha123 are easy targets for brute-force or dictionary attacks. They can often be guessed quickly because they lack both complexity and length. Common sequences such as 123 or predictable patterns are widely used and frequently appear in leaked password databases.

2. **Use a Mix of Uppercase, Lowercase, Numbers, and SpecialCharacters**
   Passwords that include a variety of character types are significantly harder to crack. For example, a password like T@u7bK$9#P!x is much stronger than a basic lowercase-only password because it includes uppercase letters, symbols, and numbers, which increases its entropy (randomness).

3. **Increase Password Length to 12 Characters or More** Length is a critical factor in password strength. Longer passwords take more time and resources to crack using brute-force methods. A password with 12 or more characters, especially when combined with complexity, is far more secure than shorter alternatives.
4. **Avoid Using Personal Information or Dictionary Words** Names, birthdates, or dictionary are vulnerable because attackers often start with these in their attack methods. Even with added numbers or symbols, these patterns remain predictable. Using random phrases or completely unrelated words with symbols and numbers is much safer.
5. **Create Unique Passwords for Every Account** Reusing the same password across multiple websites increases risk. If one site is compromised, attackers can use the stolen password to try and access your other accounts. Always generate unique, complex passwords for each service.

By following these practices, users can create passwords that are much more resistant to common attack methods and better protect their digital identities.

<u>Common Password Attacks:</u>

- Brute Force Attack: Tries every possible combination until it finds the correct one. Short/simple passwords are easy to break.

- Dictionary Attack: Uses a list of common words or phrases. Passwords like password123 or theertha123 are vulnerable.
- Credential Stuffing: Uses leaked passwords from previous breaches to access accounts.

Why Password Complexity Matters in Cybersecurity

Password complexity plays a crucial role in protecting user accounts from unauthorized access. Complex passwords are harder to guess or crack, especially when attackers use automated tools or stolen credential databases.

1. Higher Complexity = Higher Resistance

A complex password includes:

- Uppercase and lowercase letters
- Numbers
- Special characters
- Long length (12 or more characters)

The more varied and longer a password is, the more combinations an attacker must try, which increases the time, effort, and computational power needed to break it. For example, the password .T@!u7bK$e9#P@1x is considered very strong because it contains random characters, mixed cases, symbols, and is long enough to resist attacks.

2. Weak Passwords Are Easily Cracked

Passwords like theertha123 or password@123 may seem strong because they contain symbols or numbers, but they are still easily cracked by:

- Brute-force attacks (which try every combination)
- Dictionary attacks (which use common passwords/words)
- These weak passwords are usually found in leaked password lists, making them even riskier.

3. Importance of Randomness (Entropy)

Entropy refers to the unpredictability or randomness of a password. A password that follows a common pattern (like Name@123) has low entropy, meaning it's easier to guess. A truly strong password should be unpredictable, not based on personal information, and not follow obvious patterns.

By understanding and applying the principles of password complexity, users can significantly reduce the risk of unauthorized access and strengthen the overall security of their digital identities.